



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/017,230	12/07/2001	Mette Vesterager Petersen	45900-000713/US	1576
30593	7590	12/22/2005		
HARNES, DICKEY & PIERCE, P.L.C. P.O. BOX 8910 RESTON, VA 20195			EXAMINER DERWICH, KRISTIN M	
			ART UNIT 2132	PAPER NUMBER

DATE MAILED: 12/22/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 10/017,230	Applicant(s) PETERSEN ET AL.	
	Examiner Kristin Derwich	Art Unit 2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 24 August 2005.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-134 is/are pending in the application.
- 4a) Of the above claim(s) 58-73, 76 and 92-95 is/are withdrawn from consideration.
- 5) ☒ Claim(s) 118 is/are allowed.
- 6) ☒ Claim(s) 1-57, 74, 75, 77-91, 96-102, 106-117 and 119-134 is/are rejected.
- 7) ☒ Claim(s) 103-105 is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 4/23/02 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date <u>9/8/03, 3/8/02, 1/13/05</u> . | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. Claims 1-134 are pending.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

2. Claims 1-52 and 96-119 rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. The claims are directed to a method of performing numerical computations wherein the acts of the process consist only of manipulating numbers. In chapter 2106 of the MPEP, item IV, section B, item number 1, Nonstatutory Subject Matter, it states, "If the 'acts' of a claimed process manipulate only numbers, abstract concepts or ideas, or signals representing any of the foregoing, the acts are not being applied to appropriate subject matter... Thus, a process consisting solely of mathematical operations, i.e., converting one set of numbers into another set of numbers, does not manipulate appropriate subject matter and thus cannot constitute a statutory process."

3. Claims 56 and 57 rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. The claims are directed to manipulating signals. See above citation from MPEP 2106.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

Art Unit: 2132

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

4. Claims 4, 10, 11, 13, 14, 20-28, 40-44, 46, 47, 74, 75, 83, 84, 88, 102-105, 108, 109, 114-117 and 120-134 rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

As per claims 3, 4, 44:

The term "involve" in claims 3, 4 and 44 renders the claim indefinite. The term "involve" is not defined by the claim, the specification does not provide a standard for ascertaining the requisite degree of "involvement", and one of ordinary skill in the art would not be reasonably apprised of the scope of the invention. In addition, there is a lack of antecedent basis in claim 4 when referring to the step of performing computations. It depends from claim 3 which does not contain a step of *performing* computations and again the word involves is vague and indefinite. Finally, in claim 3, the computations have the decimal separators in different positions for the two different numbers, in claim 4 it states that they are in selected positions. It is unclear whether or not the different places from claim 3 are the selected positions, if they are not then claim 4 is illogical, further clarification is needed. Claims 3 and 4 are not rejected over prior art.

As per claims 10, 11, 13 and 14:

Claims 10, 11, 13 and 14 recite the limitation "mathematical system" in line 1. There is insufficient antecedent basis for this limitation in the claims. Claim 10 depends from claim 7 which includes the added limitation, "at least one of: a differential equation,

a discrete mapping", claim 10 skips the limitations of claim 7 and essentially depends from claim 1 if the mathematical system is truly what the added limitation is to be applied to and therefore there is a lack of antecedent basis with regards to claim 7. The same applies to claims 13 and 14.

As per claims 20-28, 40-43, 46, 47 and 102 - 105:

It is unclear what the scope of these claims are based on their current condition. Therefore, they cannot be examined on the merits for a prior art search since the scope is not clear, correction is required to clarify what the scope of the claims is.

As per claims 74, 75 and 120-134:

These claims lack antecedent basis since they depend from withdrawn claim 69, therefore they cannot be examined on the merits since the scope of the claims cannot be determined.

As per claim 86:

Claim 86 recites the abbreviation "i.e." which make the claim vague and indefinite. Clarification is requested as to whether what follows i.e. is meant to be an example of the claim or a part of the claim itself.

As per claim 88:

Claim 88 recites the limitation "the steps of claim 87" in line 2. There is insufficient antecedent basis for this limitation in the claim. It is unclear whether or not claim 87 is meant to include the claims it depends from.

As per claims 114-117:

The term "sufficiently" in claim 114 is a relative term which renders the claim indefinite. The term "sufficiently" is not defined by the claim, the specification does not provide a standard for ascertaining the requisite degree, and one of ordinary skill in the art would not be reasonably apprised of the scope of the invention. Clarification is requested.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

5. Claims 1, 6, 29-34, 97, 98 and 119 rejected under 35 U.S.C. 102(e) as being anticipated by Crandall, U.S. Patent No. 6,587,563.

As per claims 1 and 6, Crandall discloses a method wherein a mathematical system comprises:

A chaotic system expressed in discrete terms, the chaotic system utilizing fixed point numbers (7:39-47), obtaining from the chaotic system interim solutions used in future iterations of the system and extracting a set of data that represents a subset of digits of the resulting number (fig. 2A, 4:48-5:23). Wherein the resulting number could be expressed as either an integer, floating point or fixed point number (7:39-47).

As per claims 29-34 and 98:

Crandall discloses a method wherein a mathematical system includes a key being used to determine initial conditions of the chaotic system where the key can be a public or private key (2:20-24, 4:49-5:5).

As per claims 44 and 45:

Crandall discloses a method wherein data represents an operation on a block of plaintext in a block-cipher encryption and decryption system (9:66-10:10).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

6. Claims 15, 16, 110 and 111 rejected under 35 U.S.C. 103(a) as being unpatentable over Crandall (U.S. 6,587,563) as applied to claims 1 and 97 above and further in view of Bernstein et al. (Bernstein), U.S. Patent No. 5,007,087.

As per claims 15, 16, 110 and 111:

Crandall fails to disclose computing at least one Lyapunov exponent during the course of computations, however, Lyapunov exponents were well known in the art at the time of applicant's invention as exemplified by Bernstein in a similar field of endeavor. Lyapunov exponents needed to be calculated to confirm an equation was chaotic by being positive (5:15-33).

Art Unit: 2132

7. Claims 2, 5, 7, 8, 9, 10, 11, 12, 13, 14, 17, 99-102, 106-109, 112 rejected under 35 U.S.C. 103(a) as being unpatentable over Crandall (U.S. 6,587,563) as applied to claims 1 and 97 above and further in view of Fleming-Dahl (Fleming), U.S. Patent No. 6,744,893.

As per claims 2, 5, 7-14, 17, 99-102, 106-109 and 112:

Fleming substantially teaches a set of data resulting from a chaotic system being used as a pseudo-random number (1:17-35), at least one non-linear function governing a state variable (2:6-23), a set of non-linear ordinary differential equations which govern a state variable as a function of an independent variable (9:50-67), a set of non-linear mapping functions wherein the map comprises a Henon map (11:50-58).

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to combine the cryptographic techniques of Crandall with the communication system of Fleming since Crandall's cryptographic method would make the communication system more secure (Crandall, 1:10-14).

8. Claims 18, 19, 35-37, 39, 48, 49 and 113 rejected under 35 U.S.C. 103(a) as being unpatentable over Crandall (U.S. 6,587,563) as applied to claims 1 and 97 above and Crandall in view of Fleming (U.S. 6,744,893) as applied to claim 14 above and further in view of Carroll et al. (Carroll), Cryptologia.

As per claims 18, 19 and 113:

Carroll substantially teaches utilizing a Lorenz system as a set of differential equations (pg. 54, background).

As per claims 35 -37, 39:

Carroll substantially teaches extracting a plurality of pseudo random numbers resulting from the computation of the Lorenz system (pg. 60, 2nd paragraph). It was well known in the art at the time of applicant's invention to extract a number derived from the k least significant bits of a resulting number as demonstrated by Luyster (U.S. 6,182,216). Luyster extracts f bits from the least significant bits (8:57-64) in a similar endeavor.

As per claims 48 and 49:

Carroll substantially teaches pseudo random numbers extracted from pseudo random generators, used as or for generating keys (pg. 52, Introduction).

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to combine the pseudo random number generator disclosed by Carroll with the cryptographic method of Crandall because the sequences would produce a much stronger encryption algorithm with the use of long numbers having random characteristics since it would reduce the probability of the encryption scheme being broken by a cryptanalyst (Carroll, pg. 52, abstract).

9. Claim 50 rejected under 35 U.S.C. 103(a) as being unpatentable over Crandall (U.S. 6,587,563) as applied to claim 1 above and further in view of Hardy et al. (Hardy), U.S. Patent No. 6,079,018.

Hardy substantially teaches the use of pseudo random numbers generated to be used as digital signatures (8:4-7).

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to combine the invention of Crandall which generates pseudo

random numbers every iteration of the chaotic system as digital signatures because the chaotic system will produce highly unguessable and distinct pseudo random numbers (7:48-57).

10. Claim 51 rejected under 35 U.S.C. 103(a) as being unpatentable over Crandall (U.S. 6,587,563) as applied to claim 1 above and further in view of Moskowitz et al. (Moskowitz), U.S. Patent No. 5,889,868.

Moskowitz substantially teaches the use of pseudo random numbers used to generate watermarking key bits, which are used to watermark digital data, generated by a non-linear, chaotic, generator (3:39-45).

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to utilize the pseudo random numbers generated by the chaotic system of Crandall as watermark bits to be applied to a watermark since Moskowitz utilizes a chaotic system to generate the bits.

11. Claims 77-80, 86, 87, 96 and 114 -116 rejected under 35 U.S.C. 103(a) as being unpatentable over Fleming (U.S. 6,744,893) in view of Crandall (U.S. 6,587,563).

As per claims 77, 86, 96 and 114 -116:

Fleming substantially teaches generating a pseudo-random number by use of a chaotic system and obtaining from performing computations on the chaotic system part of a solution to the system and extracting a pseudo random number derived from a result of the system (1:17-35, 2:6-24). Fleming also shows a range for a value and if the value does not fall into the range then one is assigned (40:60-67). Fleming fails to teach defining an encryption key representing initial conditions for the system and

expressing at least one variable as a fixed point number and manipulating the original data and pseudo random number by logical operation. However, Crandall discloses utilizing a key as initial conditions for the system (2:20-24, 4:49-57), expressing a variable as a fixed point number (7:39-47) and manipulating the data and pseudo random number by logical operation in order to encrypt and decrypt subsets of the data (9:66-10:65).

As per claim 78:

Fleming and Crandall substantially teach claim 77 as disclosed above, in addition, Crandall further discloses splitting the data and the key to obtain a subset of the original data (10:26-37).

As per claims 79 and 80, Fleming and Crandall substantially teach claim 77 as disclosed above, further, claims 36 and 37 disclose similar limitations.

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to combine the cryptographic techniques of Crandall with the communication system of Fleming since Crandall's cryptographic method would make the communication system more secure (Crandall, 1:10-14).

12. Claims 81, 82 and 85 rejected under 35 U.S.C. 103(a) as being unpatentable over Fleming (U.S. 6,744,893) in view of Crandall (U.S. 6,587,563) and further in view of Rosenthal, U.S. Patent No. 5,359,659.

As per claims 81, 82 and 85:

Fleming and Crandall substantially teach claim 77 as disclosed above, Rosenthal further teaches producing multiple pseudo-random numbers and storing them as keys

Art Unit: 2132

and once a key has been exhausted, clearing out the memory to start over again (6:38-68).

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to employ utilizing multiple keys as in Rosenthal, for each message transmission in order to further guard against hackers (Rosenthal, 6:49-52).

13. Claims 83 and 84 rejected under 35 U.S.C. 103(a) as being unpatentable over Fleming (U.S. 6,744,893) in view of Crandall (U.S. 6,587,563) and further in view of Rosenthal (5,359,659) as applied to claim 82 above and further in view of Crouch et al. (Crouch), U.S. Patent No. 5,383,143.

As per claims 83 and 84:

Fleming, Crandall and Rosenthal substantially teach claim 82 as disclosed above, Crouch further teaches a method comprising:

Storing selected solutions in a linear feedback shift register that is adapted to store a finite number of solutions,

Determining if there are any duplicate solutions produced,

If a duplicate is found then a spare pseudo random number is used as the new seed,

The rest of the random numbers in the shift register are saved for future use and

The generation of pseudo random numbers continues (5:7-44).

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to combine the reseeding LFSR circuit of Crouch with the cryptographic combination made up by Crandall, Rosenthal and Fleming because it

would increase the efficiency of the pseudo random number generator in a reduced surface area (Crouch, 4:33-40)

14. Claims 89 - 91 rejected under 35 U.S.C. 103(a) as being unpatentable over Fleming (U.S. 6,744,893) in view of Crandall (U.S. 6,587,563) and further in view of Hardy et al. (Hardy), U.S. Patent No. 5,195,136.

Claims 89 - 91 are similar to claim 77, further, running an encryption system in an encryption and decryption mode was well known in the art at the time of the invention as exemplified by Hardy, 1:14-29.

15. Claim 117 rejected under 35 U.S.C. 103(a) as being unpatentable over Fleming (U.S. 6,744,893) in view of Crandall (U.S. 6,587,563) as applied to claim 114 above and further in view of Bernstein (5,007,087).

Fleming and Crandall fail to disclose computing at least one Lyapunov exponent during the course of computations, however, Lyapunov exponents were well known in the art at the time of applicant's invention as exemplified by Bernstein in a similar field of endeavor. Lyapunov exponents needed to be calculated to confirm an equation was chaotic by being positive (5:15-33).

Allowable Subject Matter

16. Claim 118 allowed.

17. Claims 103-105 objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Conclusion

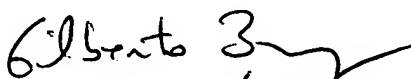
Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kristin Derwich whose telephone number is 571-272-7958. The examiner can normally be reached on Monday - Friday, 8:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).


KMD

Kristin Derwich
Examiner
Art Unit 2132


GILBERTO BARRON JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100